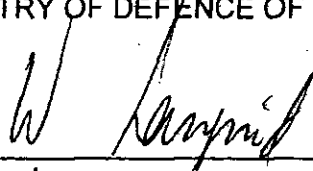


FOR THE MINISTRY OF DEFENCE OF THE KINGDOM OF NORWAY:

  
\_\_\_\_\_  
Signature

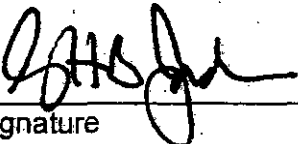
Langrud, Walther  
\_\_\_\_\_  
Name

BG NOA (RET) Director General  
\_\_\_\_\_  
Title

Baerum, NORWAY  
\_\_\_\_\_  
Location

\_\_\_\_\_  
Date

FOR THE SECRETARY OF STATE FOR DEFENCE OF  
THE UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND:

  
Signature

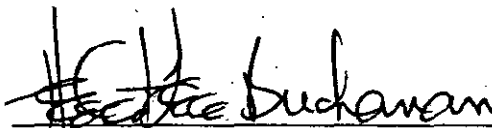
G H B JORDAN  
Name

DEPUTY UNDER SECRETARY (RESEARCH & TECHNOLOGY)  
Title

LONDON  
Location

21st Dec 2000  
Date

FOR THE SECRETARY OF DEFENSE ON BEHALF OF THE DEPARTMENT OF  
DEFENSE OF THE UNITED STATES OF AMERICA:

A handwritten signature in dark ink, appearing to read "H. Lee Buchanan", is written over a horizontal line.

Signature

H. Lee Buchanan

Name

Washington, DC

Title

Assistant Secretary of the Navy  
(Research, Development, & Acquisition)

Location

OCT 31 2000

Date

## ANNEX A: TASK DESCRIPTIONS

1. Introduction
2. System Architecture
3. Information Services
4. Management of large Networks
5. Security
6. QoS Routing
7. Mobility
8. Sub Networks
9. Directory service
- Appendix 1 INSC project schedule

## 1. INTRODUCTION

The work under the MoU will provide a demonstration of a secure, loosely coupled military internetwork, as applied to a variety of transmission media. The envisaged operational benefits which will accrue from this work are

- timely command decisions
- consistent tactical picture
- transmission of high volume surveillance information
- time-critical weapons targeting and control
- improved quality-of-life to deployed personnel (e.g. supporting email connection to family at home)

A coordinated program of work will be carried out to set up and run the demonstration. The work to be carried out under the INSC MoU is broken down into 8 tasks, as follows:

Task 1 - System Architecture

Task 2 - Information Services

Task 3 - Management of large Networks

Task 4 - Security

Task 5 - QoS Routing

Task 6 - Mobility

Task 7 - Sub Networks

Task 8 - Directory Services

It is intended that demonstrations will be coordinated with relevant NATO bodies.

The work to be carried out by the Participants under each task is described in paragraphs 2 through 8 of this Annex.

## 2. TASK 1 - SYSTEM ARCHITECTURE

### 2.1 Description

This task will develop an overall technical architecture for INSC that will consist of a system architecture, a test architecture and a demonstration architecture. The technical architecture will define the way in which the products of tasks 2 to 8 are to be integrated. The task will also carry out the overall co-ordination and planning of the INSC Project. It will provide reporting and dissemination of the results of INSC during and upon completion of the Project.

### 2.2 Products

The following deliverables will be provided:

Design:

- Project plan and work breakdown structure
- System architecture description

Implementation:

- System simulation

Test:

- System integration plan
- System test plan
- Performance evaluation of information services over an INSC subnetwork, including
  - ♦ Evaluation of the impact of security services on end-to-end service quality and interoperability
  - ♦ Demonstration of the viability and benefits of dynamic routing and multicasting in an IPv6 environment
  - ♦ Evaluation of mechanisms to support mobility in a military environment.
- System demonstration plan
- INSC final report

### 3. TASK 2 - INFORMATION SERVICES

#### 3.1 Description

The objective of the task Information Services is to investigate and demonstrate how military-applicable information services can be supported by and benefit from the technologies and concepts that are to be studied through the INSC Project (e.g., improved responsiveness to the user needs).

The Information Services task can also be used to assist test activities of other INSC tasks, namely, system architecture, security, management, QoS routing, directory services, mobility and subnetworks and to exploit the potential of the INSC communications network, which consists of different types of military and civilian subnetworks as described in paragraph 8.1 of this Annex.

#### 3.2 Products

Identification and performance evaluation of a set of representative military-applicable information services that may include:

- Packetized voice
- Messaging with military features (e.g. multicasting and radio silence functionality, PCT (digital signature)), based on SMTP and X.400
- Reliable Multicast File distribution, including images and graphics
- WWW access and browsing, including server and client aspects
- Multimedia conferencing, including whiteboard and other cooperative planning tools
- Time critical sensor application

This task includes identification of transport and network layer protocols for each selected information service. It also specifies QoS requirements in conjunction with tasks 5 and 7.

#### 4. TASK 3 - MANAGEMENT OF LARGE NETWORKS

##### 4.1 Description

Network Management is an important aspect of operational networks, composed of heterogeneous sub-networks in a national or multi-national environment.

The principal objective of this task is to develop and demonstrate an effective network management capability for a mosaic of independently developed subnetworks each with its own network management paradigms and local management entities, many of which may be incompatible with those in other subnetworks.

To achieve this objective the management capability must include, but is not necessarily limited to the following technical capabilities in an environment of multiple heterogeneous management domains:

- management over low-bandwidth subnetworks using intelligent agents
- distributed and/or peer-to-peer management
- management of mobile communication resources and users
- management of security

##### 4.2 Products

- Definition of a management functionality (including management of security issues) and policy for a loosely coupled internetwork based on dissimilar subnetwork management policies, including the mapping of an INSC management policy and involved national management policies
- Definition of a minimum set of management information to be provided by non-cooperative subnetworks.
- Definition of access control methods for peer and multi-ownership management elements
- Specification of the functionality of intelligent agents
- Validation of the INSC management architecture using simulation tools
- Realization and testing of the INSC management model based on available management components, including management of mobile networks



## 5. TASK 4 - SECURITY

### 5.1 Description

Interconnecting heterogeneous networks for military use, including commercial services, requires that security be taken into account. For the purpose of making military networks secure, bulk encryption is not always possible nor sufficient. Network as well as application layer security mechanisms have to be considered.

Network layer security efforts will be conducted in order to determine whether the security features of the forthcoming IPv6 are adequate for military requirements. Other solutions or enhancements may have to be investigated or explored.

User authentication requires that security at the application layer be addressed. This is especially important for secure management.

The operational impact of the potential solution(s) will be assessed.

The task does not cover specific cryptographic algorithms.

### 5.2 Products

- Specification of a functional profile for IPSec
- Implementation of the specified functional profile
- Definition of test procedures for IPSec
- Evaluation and testing of the performance and robustness of the various IPSec implementations
- Specification of the functionality of security enhanced application layer security protocols
- Selection, implementation and testing of security enhanced application layer security protocols
- Evaluation of the dependencies between security functionality at the network layer and security enhanced application layer security protocols

## 6. TASK 5 - QoS - ROUTING

### 6.1 Description

To provide effective performance in a military internetwork, especially in a bandwidth-limited environment, the network layer should respond to the Quality of Service requirements of individual information flows. Current IP router networks have limited capability in this area. QoS parameters may include timeliness, priority, reliability, security and cost. The task will assess the appropriateness for military purposes of emerging technologies, in areas such as:

- resource reservation protocols to support high priority traffic (e.g. RSVP)
- scheduling protocol to provide fair allocation of resources
- flow labelling in IPv6 to identify particular QoS requirements
- a common definition of QoS parameters across different subnetworks
- exchanging of QoS information between subnetworks, routers and applications
- mechanisms for enforcing priority within the network
- mechanisms or procedures for common definition of users' QoS requirements
- unicast and multicast routing protocols for IPv6

### 6.2 Products

- definition of a set of selected QoS parameters and parameter values for usage across a variety of subnetworks, including a security parameter (e.g. using defined transmission paths for sensitive information)
- Specification of procedures and mechanisms facilitating QoS information passing between sub network, router and application
- test and evaluation of reservation, scheduling and priority mechanisms
- test and evaluation of routing protocols
- test and evaluation of QoS routing under dynamic network topology

## 7. TASK 6 - MOBILITY

### 7.1 Description

Mobility is essential in military operations. This task investigates the applicability of civil Internet technologies to dynamic military networks. Enhancements will be developed where civil technologies prove inadequate for mobile military networks.

To support mobility of end systems, mobile IP will be evaluated for adequacy in military networks.

For dynamic network topologies (e.g. mobile routers and end systems within the area of operation), stable civil standards are not available. Work will be carried out to enhance existing protocols, and where necessary develop new protocols appropriate for dynamic military networks.

### 7.2 Products

- Definition of test scenarios for mobile IP
- Test and evaluation of the adequacy of mobile IP for military end systems
- Integrate and test selected functions in mobile IP for military end systems
- New or enhanced routing algorithms for mobile networks
- Dynamic DNS (Domain Name Server) for mobile networks

## 8. TASK 7 - SUB NETWORKS

### 8.1 Description

The objective is to demonstrate the integration of commercial and military subnetworks into an INSC-like configuration based on an IP-to-subnetwork interface to be specified or developed. The INSC configuration may include both wired and wireless subnetworks, such as:

- ISDN
- ATM
- SATCOM
- HF
- 6Bone/Internet
- wireless LAN

### 8.2 Products

- Specification and installation of the defined, common IP-to-subnetwork interface, including the mapping of QoS parameters
- Evaluation of the ability of the subnetworks in combination with IPv6 to support guaranteed QoS, priority transmission and graceful degradation when operating under different network conditions (via simulation or testbed)
- Adaptation of national sub networks to the INSC specified common IP-to-subnetwork interface.

## 9. TASK 8 - DIRECTORY SERVICE

### 9.1 Description

The objective of this task is to provide a directory service to support the operation of the INSC network. It is intended that the directory service will support network configuration, mobility, security and management.

### 9.2 Products

- Specification of the service and sub schema requirements to support network configuration, mobility and management
- Implementation of the required service and sub schema
- Implementation of a X.509 based public key infrastructure for supporting security within Task 4